



SECURITY AWARENESS NEWSLETTER

September 2002

<u><i>Combat SPAM</i></u>	<u><i>Anti-Virus Information</i></u>	<u><i>Homeland Security Conferences</i></u>
<u><i>Manage Junk and Adult-Content E-Mail</i></u>	<u><i>Passwords</i></u>	<u><i>Microsoft Information</i></u>
<u><i>Configure Privacy Settings</i></u>	<u><i>Hacker Information</i></u>	<u><i>Useful URL's</i></u>

INTRODUCTION

In an effort to emphasize the importance of security issues to all staff and to promote security awareness, the GOT Division of Security Services is pleased to provide this security awareness newsletter. It is hoped that the information contained herein will provide practical tips, security solutions, and job-saving techniques.

Also, as a friendly reminder, GOT staff are encouraged to familiarize themselves with all policies, manuals, and procedures which can be found at [GOT Policies and Procedures](#).

[Back to Top](#)

COMBAT SPAM

What Exactly is SPAM?

If you have ever received unsolicited commercial e-mail, you have been spammed. Spam kills legitimate messages, wastes our valuable time, and compels businesses to buy excess equipment to cope with spam-driven mail surges.

Have you seen the "We will email your ad to 1 million people for \$99!" promotions online? You may have seen similar ones on the web, or perhaps you have received promos for them in your in-box. There are individuals and companies who send spam for a living.

What customers of these "bulk email senders" don't realize is that sending spam to promote their product or service does more harm than good. All they see is the "low cost advertising" promotion, and they are hooked. What they are not told is that they will receive tons of nasty e-mail and postal letters, be reported to their ISP (Internet Service Provider) risking losing their access, have their domain blacklisted, possibly be reported to the Federal Trade Commission (FTC), and give an overall negative image of their product/service.

Combating SPAM:

1. Use your business e-mail account for regular business purposes, and a personal e-mail account for giving out online (e. online shopping, website forms, posting to newsgroups -- basically, anything that you have to "sign up" for.)
2. Before signing up for something online, if you see a 'privacy policy' posted, read it. Find out if they are going to share or sell your address. If there is not a policy posted, first decide if you trust that site before giving out your address.
3. Do not reply to or acknowledge any SPAM you receive. Do not click on the links they provide no matter how tempting. Deny them the satisfaction. If you like what they are offering, go to a search engine and find a similar company with a similar service that didn't send the SPAM.
4. Don't provide your e-mail address on your website. There are bots that constantly surf the web harvesting e-mail addresses. We realize this isn't ideal for everyone, so if you do want your e-mail address on your site, you may want to turn it into a graphic instead (bots can't read the text on graphics), or use a non plain-text version of the e-mail posted (ascii codes are roughly 80 percent effective).
5. Do not respond to "REMOVE ME FROM YOUR LIST" feature. All that will do is let the sender know your e-mail address is active and your name will be resold again, and again.
6. Report spam by completing GOT-F012, which can be found at http://www.state.ky.us/got/ois/security/Security_forms.htm SPAM can also be reported to the Federal Trade Commission (FTC) by sending them the entire message, including the full header. If you have a specific complaint about spam, complete the form at [https://rn.ftc.gov/dod/wsolicq\\$.startup?Z_ORG_CODE=PU01](https://rn.ftc.gov/dod/wsolicq$.startup?Z_ORG_CODE=PU01) You also can forward spam directly to the Commission at UCE@FTC.GOV without using the complaint form



[Back to Top](#)


MANAGE JUNK AND ADULT CONTENT E-MAIL THROUGH OUTLOOK

Outlook can search for commonly used phrases in e-mail messages and automatically move these messages to a junk email folder in your Inbox, to your Deleted Items folder, or to any other folder you specify.

You can also filter messages with a list of senders of junk and adult content e-mail. As you receive unwanted e-mail messages, you can create a list of the e-mail addresses of these senders.

Note: Make sure that when you first begin using these features that you review messages that are automatically removed from the Inbox to ensure that any wanted messages are not accidentally removed.

To automatically move junk mail from your Inbox:

- On the standard toolbar, click the Organize button 
- Click Junk E-Mail.
- In the bulleted items for Junk and for Adult Content messages, in each of the first lists, click move. When you click move, the second list on each line will change from a list of colors to a list of folder destinations.
- You can leave the default destination Junk E-Mail or choose Deleted Items or Other folder.
- Click Turn On to enable the feature.

To filter out senders of junk E-mail and adult content:

- Click on the Organize button.
- Click Junk E-Mail.
- Click the underlined phrase [click here](#).
- In the second bulleted item, click Edit Junk Senders or Edit Adult Content Senders.
- Click ADD to add an E-mail alias or a domain of a sender. You can also review, edit, or delete entries from the list.

In addition to using the built-in Outlook filters, you can create custom rules to filter out specific types of unwanted messages. Custom rules include additional words or phrases that are not included in the Filters.txt file.* Just as with the built-in feature, you can specify that the rules you create move messages from your Inbox to the junk e-mail folder, Deleted Items folder, or to any other folder you specify.

To create custom rules:

- On the Tools menu, click Rules Wizard, and then follow the instructions on your screen.

*If you're interested in what terms Outlook uses to filter suspected junk e-mail messages look in a file called Filters.txt, located in the C:\Program Files\Microsoft Office\Office10\LocaleID folder, where LocaleID is the locale identifier (LCID) for your installation of Microsoft Office. For example, the LCID for English - United States is 1033. For a list of LCIDs, see Microsoft Office Help.

[Back to Top](#)

CONFIGURE PRIVACY SETTINGS THROUGH INTERNET EXPLORER

You can configure your privacy settings in Internet Explorer 6 by clicking Internet Options on the Tools menu, and then clicking the Privacy tab. These settings replace the cookies settings on the Security tab in Internet Explorer 4 and 5 (and the Advanced tab in Internet Explorer 3). Of the six Privacy settings below, GOT recommends the "Medium High" setting:



- **Block All Cookies:** Select this setting to prevent websites from sending cookies to your PC and reading any cookies that were saved during previous visits. Note that websites that use cookies for e-commerce transactions, personalization, graphics, or other interactive features will not function properly with this setting.
- **High:** Select this setting to keep out all cookies that do not have compact privacy policies. This setting also blocks cookies from all websites that may use your information for marketing or transfer it to other third party websites. Note that websites that use cookies for e-commerce transactions, personalization, graphics, or other interactive features will not function properly with this setting.
- **Medium High:** Select this setting to block cookies from third party websites that do not have compact privacy policies. This setting also blocks cookies from all websites that may use your information for marketing purposes or transfer it to other third party websites.
- **Medium (default level):** Select this setting to block cookies that are sent from websites beyond the site that you are accessing (third party websites) that do not have compact policies.
- **Low:** Select this setting to accept all cookies from websites you are accessing. It restricts cookies from third party websites by deleting them from your PC after you close Internet Explorer 6.0.
- **Accept All Cookies:** Select this setting to accept all cookies regardless of their origin. This setting will not alert or allow web users to block any cookies that gather information on them.

NOTE: Changing your privacy preferences does not affect the cookie acceptance policy for cookies that have already been set unless you move the slider to Accept All Cookies or Block All Cookies.

For more information regarding configuring privacy settings in IE, visit the Microsoft website at <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxp/pro>

[Back to Top](#)

ANTI-VIRUS INFORMATION -- FEELING LUCKY??



If you're not taking precautions to protect your data from computer viruses, you're simply relying upon luck -- luck that just may run out soon.

There are thousands of viruses in existence, with several hundred being discovered each month.

The good news is that it's relatively easy to safeguard your data from most viruses. In fact, this protection is easier than you might think. It's simply a matter of recognizing the sources of infection, using your anti-virus software diligently, and knowing what to do when a virus is detected.

Common sources of virus infection include files downloaded from the Internet, e-mail attachments, files brought in from home computers, and even shrink-wrapped software. Whenever you receive files from such sources, always be sure to use your anti-virus software to scan the files before using them.

If your software detects a virus, don't panic. Be sure to report the incident immediately to your systems administrator so the source can be traced and anyone else who may have received the virus can be alerted. If you don't, it just might find its way back to you!

So even if you are feeling lucky, please follow the guidelines below to help make sure we do not fall victim to destructive computer viruses:

- Always use current anti-virus software on your office and home computers.
- Scan all files downloaded from the Internet.
- Don't open any e-mail attachments that look suspicious or come from unknown senders. Be on the lookout for e-mails from people you know, but with language or style they wouldn't normally use--this should raise a red flag. If you decide to open the attachment, be sure to scan it first.
- Disable the auto preview feature in Microsoft Outlook, if you are using an older browser than Internet Explorer 6
- Be very careful if a virus warning encourages you to delete files from your system; the originator of the message may be trying to trick you into deleting valid files.
- Scan diskettes and CDs before use.
- Remember, whenever there's a doubt, scan it! Also, if you're not sure about something, or have even the slightest concern, check with your systems administrator

before taking action.

- Report all virus incidents to your systems administrator as soon as possible.

Note for Windows XP and Me Users: If you use Windows XP or Me, you have to disable System Restore before you remove a virus. These operating systems will bring the virus back from the dead if you don't turn off this "safety" feature before you disinfect.

[Back to Top](#)

PASSWORDS

If you use a password to access any computer or Internet services, make sure that they are hard to guess and keep them to yourself. Also, use different passwords for different things. If someone guesses a password for one, you don't want them to have access to all those services. Never give out your password to anyone!

One strategy for creating and remembering passwords is to come up with a phrase that only you would remember. For example, the phrase "I was married on June 6 in Frankfort," would result in a case sensitive password of 'Iwmo#J6iF' by using the first letter of each word in the phrase and separating it with a special symbol. For a list of the Division of Security Services' Password Creation Tips, see

<http://www.state.ky.us/got/ois/security/Password%20Creation%20Tips.htm>

[Back to Top](#)

HACKER INFORMATION

Ethical Hacker Faces War Driving Charges:

A Houston computer security analyst has been charged with hacking after demonstrating the insecurity of a county court's wireless LAN. Stefan Puffer, 33, was indicted by a Grand Jury on Wednesday with two counts of fraud for allegedly breaking into Harris County district clerk's wireless computer system. It's believed to be the first case of its kind in the United States.

DrinkOrDie Member Gets 33 Months in Prison:

A 24-year-old member of DrinkOrDie, one of the oldest international piracy groups on the Internet, has been sentenced to 33 months in federal prison for conspiring to violate criminal copyright laws.

Christopher Tresco of Allston, Mass., pleaded guilty in May in U.S. District Court for the Eastern District of Virginia of using his employer's computers to distribute copyrighted material, including movies, software, games and music, according to a U.S. Department of Justice statement.



Israeli Teens Charged in Goner Case:

Five Israeli teenagers have been charged in Haifa District Court with willfully causing damage to computers for their roles in creating the Goner virus. One of the five is charged with actually writing the virus; the others are charged with spreading it. The Goner virus arrives in the guise of an attached screensaver and shuts down firewalls and anti-virus software running on infected computers. For more information, see <http://news.com.com/2100-1001-948596.html>

Telecom Hacker Charged:

A 22-year-old Sydney man has been charged with "unauthorized modification of data with intent to cause impairment to a computer." The man allegedly accessed the accounts of more than 400,000 Optus dial-up Internet customers; his arrest is the result of a six-month investigation.

Mitnick Writes New Security Book:

Kevin Mitnick has written a book, entitled The Art of Deception, which he hopes to have published by the end of the year.



In the book - supposedly fictional - a self-confessed superhacker describes more than a dozen scenarios where savvy hackers con network administrators into revealing passwords, encryption keys. Unconfirmed reports suggest that the book is now being carefully screened by his publishers for any hint of a real-life security snafu that has occurred in hacking history.

Mitnick, now aged 38, served five years in a U.S. federal prison for stealing software, as well as altering data on computer systems operated by a number of high profile companies, including Motorola, Novell, Nokia and Sun Microsystems. He was released in January, 2000 but under the terms of his probation cannot use a computer connected to the Internet until January of next year.

Hackers Face Stiffer Penalties:

The U.S. judicial system has become more aggressive in prosecuting cyber criminals. The passage of the Patriot Act increased the maximum sentence for breaking into a computer from five to ten years in prison, and the Cyber Security Enhancement Act could bring a hacker life in prison for recklessly causing or attempting to cause death.

[Back to Top](#)

HOMELAND SECURITY CONFERENCES

Governor's Executive Summit on Homeland Security:

The Governor's Executive Summit on Homeland Security will be held on Wednesday, November 20, 2002, 8:00 a.m. - 4:00 p.m. CST, at the Executive Inn in Owensboro, Kentucky. The meeting is for executive-level state, county and city government leaders and leaders of professional organizations who influence homeland security efforts. The summit will educate and prepare attendees on preventing terrorist activities and developing protective measures to protect our communities. The cost of the conference is \$40. For more information, contact Shirley Rodgers, Executive Assistant, Governor's Office for Technology, at 502-564-1209 or shirley.rodgers@mail.state.ky.us.

KLTPRC Conference on Homeland Security:

The Kentucky Long-Term Policy Research Center's (KLTPRC) ninth conference, "Living in a Changed World: Assessing the Homeland Security Threat," will provide information relating to long-term implications for Kentucky. It will be held on November 21, 2002, at the Executive Inn Rivermont in Owensboro, Kentucky. KLTPRC invites you to join fellow Kentuckians from across the Commonwealth for discussions about the after effects of 9-11 and possible responses from national experts and other leaders about trends and future prospects. Learn what some are doing to "take back the night," emerge stronger and more capable of facing the uncertainty that lies ahead, meet future challenges, seize new opportunities, and thrive in the face of it all. The featured speaker will be Dr. Bruce Hoffman, International Terrorism Expert and Vice President for External Affairs for RAND. You may register at <http://www.kltprc.net/conference2002.htm> If you have questions, please contact [Billie Sebastian](#).

[Back to Top](#)

MICROSOFT INFORMATION

Outlook Meeting Request Advisory:

Most agencies fully utilize the capabilities of Microsoft Outlook's Calendar module by allowing its employees view access to all users' calendars, which is an appropriate and effective means of scheduling various business activities. However, many agencies may not be aware that Outlook Calendar also makes Outlook meeting requests and their attachments that are posted to the calendar available to be read by everyone. So use caution when including attachments of a sensitive nature in your meeting requests for they can be read by those other than originally intended.

Microsoft Vulnerability Which Can Bypass the Same Origin Policy

In Microsoft Internet Explorer 6.0, a vulnerability exists which can bypass the same origin policy. Attackers can use this to steal web cookies, gain access to local files, access object such as MSN contacts, and many other scenarios are possible. At this time **Microsoft has not released a patch** and the suggested mitigating strategy is disabling active content and

script code.

Microsoft Released Cumulative Patch for Multiple Vulnerabilities in Internet Explorer

Microsoft has released a security bulletin describing multiple vulnerabilities in Internet Explorer 5.01, 5.5 and 6.0:

- The first issue is a buffer overflow in the Gopher protocol handler. Exploitation will allow arbitrary code to be executed with the privileges that the affected product is run with.
- The second issue is described to be a buffer overflow in an ActiveX component used to display specially formatted text.
- The third issue reportedly allows a remote attacker to exploit the browser to read XML data that is located in a known location.
- The fourth issue is in how Internet Explorer displays download dialogues to users.
- The fifth issue may allow remote attackers to gain unauthorized access to local resources on client systems and perform actions such as the execution of local binaries.
- The sixth issue is a variant of the issue described in Microsoft Security Bulletin MS02-023. It may potentially allow an attacker to cause malicious script code and HTML to execute with the relaxed restrictions associated with the Local Computer Zone.

For more information, see <http://www.microsoft.com/technet/security/bulletin/MS02-047.asp>

Microsoft released MS02-043 ("SQL Server cumulative patch")

This cumulative patch fixes all known problems to date in MS SQL Server 7.0 and 2000 as well as in MSDE 1.0 and 2000. It also fixes a new bug, whereby an attacker capable of running stored procedures can execute arbitrary SQL with administrative privileges. FAQs and patch are available at <http://www.microsoft.com/technet/security/bulletin/MS02-043.asp>

[Back to Top](#)

USEFUL URL's

<http://www.fedcirc.gov/>

The Federal Computer Incident Response Center (FedCIRC) is the central coordination and analysis facility dealing with computer security-related issues affecting the civilian agencies and departments of the federal government. FedCIRC's incident response and advisory activities bring together elements of the Department of Defense (DOD), Law Enforcement, Intelligence Community, Academia and computer security specialists from Federal Civilian Agencies and Departments forming a multi-talented virtual security team.

<http://www.infosecnews.com/>

SECURITY AWARENESS NEWSLETTER

This on-line news service is backed by SC Magazine - the largest circulation information security magazine. It is read in more than 50 countries around the world and is published in three separate editions in North America, Europe and the Asia Pacific region. The news service gathers information globally through a network of correspondents and over 200 news services. Key links associated with the news direct you to further sources of information relevant to the news item being reported.

www.incidents.org

Incidents.org is a virtual organization of advanced intrusion detection analyst experts and forensic incident handlers from across the globe. The organization's mission is to provide real time driven security intelligence and support to both organizations and individuals.

www.sans.org

The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization through which more than 96,000 system administrators, security professionals, and network administrators share the lessons they are learning and find solutions to the challenges they face.

<http://www.computerworld.com/>

Computerworld continually provides IT leaders with a host of targeted information services including their award-winning newspaper, web site, email newsletters, events and books. What's more, they provide unmatched reach to IT leaders with targeted advertising and sponsorships.

<http://www.nipc.gov/about/about.htm>

Located in the FBI's headquarters building in Washington, D.C., the NIPC brings together representatives from U.S. government agencies, state and local governments, and the private sector in a partnership to protect our nation's critical infrastructures.

Established in February 1998, the NIPC's mission is to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures. These infrastructures, which include telecommunications, energy, banking and finance, water systems, government operations, and emergency services, are the foundation upon which our industrialized society is based.

[Back to Top](#)

Works Cited:

A portion of the material was provided by staffs of Infosecurity NEWSwire, ComputerWorld Security, and Security Awareness, Inc.